Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

- Free Host Shop Website Generator Remote Vulnerabilities
- FtpLocate Arbitrary Command Execution
- Greasemonkey Multiple Remote Information Disclosure
- PHP TopSites Authentication Bypass
- **Mozilla Firefox Multiple Vulnerabilities (Updated)**
- Mozilla Firefox Weak Authentication
- **Mozilla Suite / Firefox Multiple Vulnerabilities (Updated)**
- **Mozilla Suite And Firefox DOM Property Overrides (Updated)**
- **Mozilla Suite/Firefox JavaScript Lambda Information Disclosure (Updated)**
- **Multiple Vendor Telnet Client Information Disclosure (Updated)**
- **Multiple Vendors Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows (Updated)**
- Multiple Vendors MediaWiki Remote Cross-Site Scripting
- **Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service (Updated)**
- **MySQL 'mysql_install_db' Insecure Temporary File Creation (Updated)**
- NETonE phpBook Cross Site Scripting
- Oray PeanutHull System Privileges
- PHP FirstPost Arbitrary Command Execution
- PHP Surveyor Multiple SQL Injection, Cross-Site Scripting & Path Disclosure
- PHPFinance Inc.login.PHP Authentication Bypass
- PHP-Fusion BBcode 'Color' Tag Code Injection
- PHPNews 'Auth.PHP' SQL Injection
- PHPSiteSearch 'Search.PHP' Cross-Site Scripting
- Beehive Forum SQL Injection or Cross Site Scripting
- Pyrox Search 'Newsearch.PHP' Cross-Site Scripting
- RealChat User Impersonation
- Internet Graphics Server Directory Traversal
- Sendcard SQL Injection
- Siemens Wireless Router Denial Of Service
- Tim Hoeppner Ultimate PHP Board Multiple Cross-Site Scripting
- Xerox MicroServer Web Server Multiple Vulnerabilities

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Wireless

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Alwil Software Avast! Antivirus V Home/Pro 4.6691, Server 4.6.489, Client 4.6.394	A buffer overflow/ directory traversal vulnerability has been reported in Avast! Antivirus (UNACEV2.dll) that could let remote malicious users write files or execute arbitrary code. Vendor updates available:	Avast! antivirus Arbitrary Code Execution CAN-2005-2384	High	Secunia, Advisory: SA15776, July 21, 2005

	http://www.avast.com/ Currently we are not aware of any exploits for this vulnerability.	CAN-2005-2385		
Ares V1.1	A buffer overflow has been reported in Ares that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Ares Arbitrary Code Execution	High	Security Focus, 14377, July 25, 2005
Elemental Software CartWIZ V1.20	A vulnerability has been reported in CartWIZ that could let remote malicious users perform cross site scripting. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CartWIZ Cross Site Scripting CAN-2005-2386	High	Security Focus, 14386, July 26, 2005
FTPShell FTPShell Server V3.38	A vulnerability has been reported in FTPShell that could allow remote malicious user perform a denial of service. No workaround or patch available at time of publishing. Exploit scripts have been published.	FTPshell Server Denial of Service	Low	Secunia, Advisory: SA16189, July 26, 2005
GoodTech Systems GoodTech SMTP Server V5.16	A buffer overflow vulnerability has been reported in GoodTech SMTP Server (RCPT TO command) that could let remote malicious users execute arbitrary code. Upgrade to version 5.17: http://www.goodtechsys.com/smtpdnt2000.asp There is no exploit code required; however, Proof of Concept exploits have been published.	GoodTech's SMTP Server Arbitrary Code Execution CAN-2005-2387	High	SecurityTracker Alert ID: 1014561, July 24, 2005
Key Focus KF Web Server V2.5.0	A vulnerability has been reported in KF Web Server that could let remote malicious users disclose directory listings. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	KF Web Server Directory Listings Disclosure	Low	SecurityTracker Alert ID: 1014559, July 22, 2005
Microsoft JView Profiler	A vulnerability has been reported in JView Profiler that could let remote malicious users execute arbitrary code. Vendor updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-037.mspx **V1.1: JView Profiler FAQ concerning Javaprxy.dll detection, and update of title reflect all supported versions of Windows 2000.** There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft JView Profiler Arbitrary Code Execution CAN-2005-2087	High	Microsoft Security Bulletin MS05-037, July 12, 2005 USCERT, Vulnerability Note VU#939605, July 12, 2005 **Microsoft Security Bulletin MS05-037 V1.1, July 20, 2005**
Microsoft Windows Color Management Module	A vulnerability has been reported in Windows Color Management Module that could let remote malicious users cause a buffer overflow, execute arbitrary code, or take complete control of a system. Vendor updates available: http://www.microsoft.com/technet/security/bulletin/ms05-036.mspx **V1.1: Restart requirement information updated.** **Currently we are not aware of any exploits for this vulnerability.**	Microsoft Windows Color Management Module Buffer Overflow or Arbitrary Code Execution CAN-2005-1219	High	Microsoft Security Bulletin MS05-036, July 12, 2005 USCERT, Vulnerability Note VU#720742, July 12, 2005 **Microsoft Security Bulletin MS05-036 V1.1, July 20, 2005**
Microsoft Windows USB Driver	A buffer overflow vulnerability has been reported in Windows USB Driver that could allow local malicious users to execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows USB Driver Buffer Overflow CAN-2005-2388	High	Security Focus, 14376, July 25, 2005
SPIDynamics WebInspect V5	A vulnerability has been reported in WebInspect that could let remote malicious users perform cross site scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	WebInspect Cross Site Scripting	High	Secunia Advisory: SA16191, July 26, 2005
Veritas NetBackup V5.1	A vulnerability has been reported in NetBackup that could let local malicious users perform a denial of service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Veritas NetBackup Denial of Service CAN-2005-2389	Low	Secunia, Advisory: SA16187, July 25, 2005
WhitSoft Development SlimFTPd V3.16	A buffer overflow vulnerability has been reported in SlimFTPd (List, Dele and Rnfr commands), that could let remote malicious users execute arbitrary code.	SlimFTPd Arbitrary Code Execution	High	Secunia, Advisory: SA16177, July 22, 2005

	Upgrade to version 3.17: http://www.whitsoftdev.com/slimftpd/ There is no exploit code required.	CAN-2005-2373		

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Clam AntiVirus V0.86.1	Multiple vulnerability have been reported in Clam AntiVirus that could let remote malicious users cause a denial of service. Upgrade to version 0.86.2: http://www.clamav.net/ stable.php#pagestart Currently we are not aware of any exploits for this vulnerability.	Clam AntiVirus Multiple Vulnerabilities	Low	Secunia, Advisory: SA16180, July 25, 2005
Dnsmasq Dnsmasq 2.0-2.20	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to an off-by-one error when reading the DHCP lease file, which could let a remote malicious user cause a Denial of Service; and a vulnerability has been reported when receiving DNS replies due to insufficient validation, which could let a remote malicious user poison the DNS cache. Upgrades available at: http://www.thekelleys.org.uk/ dnsmasq/ dnsmasq-2.21.tar.gz Gentoo: http://security.gentoo.org/ glsa/glsa-200504-03.xml **Slackware:** **ftp://ftp.slackware.com/** **pub/slackware/slackware** Currently we are not aware of any exploits for these vulnerabilities.	Dnsmasq Multiple Remote Vulnerabilities CAN-2005-0876 CAN-2005-0877	Medium	Security Focus, 12897, March 25, 2005 Gentoo Linux Security Advisory, GLSA 200504-03, April 4, 2005 **Slackware Security Advisory, SSA:2005-201-01, July 21, 2005**
Domain Name Relay Daemon V2.19	A buffer overflow vulnerability has been reported in Domain Name Relay Daemon (DNRD) that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Domain Name Relay Daemon Arbitrary Code Execution CAN-2005-2315 CAN-2005-2316	High	SecurityTracker, Alert ID: 1014557, July 22, 2005
Eric Raymond Fetchmail 6.2.5	A remote buffer overflow vulnerability has been reported in the POP3 client due to insufficient boundary checks, which could let a malicious user obtain elevated privileges. Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/ Redhat: http://rhn.redhat.com/errata/ RHSA-2005-640.html Ubuntu: http://www.ubuntulinux.org/ support/ documentation/ usn/usn-153-1 Gentoo: http://www.gentoo.org/security/ en/glsa/glsa-200507-21.xml Currently we are not aware of any exploits for this vulnerability.	Fetchmail POP3 Client Buffer Overflow CAN-2005-2355	Medium	Fedora Update Notifications, FEDORA-2005-613 & 614, July 21, 2005 Redhat Security Advisory, RHSA-2005:640-08, July 25, 2005 Ubuntu Security Notice, USN-153-1, July 26, 2005 Gentoo Security Advisory, GLSA 200507-21, July 25, 2005
FreeBSD FreeBSD 5.3, 5.4	A vulnerability was reported in FreeBSD in the devfs(5) device file system due to insufficient validation of the node type parameter when a device is created, which could let a malicious user obtain ROOT access. Patches available at: ftp://ftp.FreeBSD.org/pub/ FreeBSD/CERT/patches/ SA-05:17/devfs.patch Currently we are not aware of any exploits for this vulnerability.	FreeBSD devfs Ruleset Bypass CAN-2005-2218	High	FreeBSD Security Advisory, FreeBSD-SA-05:17, July 20, 2005

Gentoo Sandbox	Multiple vulnerabilities have been reported in Sandbox that could allow a local malicious user to create temporary files. Update available: http://www.gentoo.org/security/en/glsa/glsa-200507-22.xml There is no exploit code required.	Gentoo Sandbox File Creation	Medium	Gentoo Security Advisory, GLSA 200507-22, July 25, 2005
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-378.html** There is no exploit code required.	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 **RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005**

GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.009-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1** Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.009, June 10, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 **Sun(sm) Alert Notification** **Sun Alert ID: 101816, July 20, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005

	TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip/gzip **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1** There is no exploit code required.			Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 **Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005**
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SGI: http://www.sgi.com/support/security/ **F5:** **http://tech.f5.com/home/bigip/solutions/advisories/sol4532.html** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Fedora Update Notification, FEDORA-2005-471, June 27, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 **Secunia Advisory: SA16159, July 21, 2005**
Hobbit Monitor V4.0.4	A vulnerability has been reported in Hobbit Monitor that could let local malicious users perform a denial of service. Upgrade to version 4.1.0: http://sourceforge.net/projects/hobbitmon/ Currently we are not aware of any exploits for this vulnerability.	Hobbit Monitor Denial of Service	Low	Secunia, Advisory: SA16179, July 25, 2005

KDE KDE 3.4, 3.3-3.3.2, 3.2-3.2.3	A vulnerability has been reported in KDE Kate and KWrite because backup files are created with default permissions even if the original file had more restrictive permissions set, which could let a local/remote malicious user obtain sensitive information. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	KDE Kate, KWrite Local Backup File Information Disclosure CAN-2005-1920	Medium	Security Tracker Alert ID: 1014512, July 18, 2005 Fedora Update Notification, FEDORA-2005-594, July 19, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:122, July 20, 2005**
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3; IPCop 1.4.1, 1.4.2, 1.4.4, 1.4.5	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-06.xml Mandriva: http://www.mandriva.com/security/advisories IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:10/tcpdump.patch Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-137_RHSA-2005-417_RHSA-2005-421.pdf TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **F5:** **http://tech.f5.com/home/bigip/solutions/advisories/sol4809.html** Exploit scripts have been published.	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 Fedora Update Notification, FEDORA-2005-351, May 3, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Ubuntu Security Notice, USN-119-1 May 06, 2005 Gentoo Linux Security Advisory, GLSA 200505-06, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:087, May 12, 2005 Security Focus, 13392, May 12, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:10, June 9, 2005 Avaya Security Advisory, ASA-2005-137, June 13, 2005 Turbolinux Security Advisory, TLSA-2005-63, June 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 **Security Focus, 13392, July 21, 2005**

Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107, 105	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-13.xml Mandriva: http://www.mandriva.com/security/advisories **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/universe/libn/** There is no exploit code required.	Multiple Vendors TLS Plaintext Password CAN-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-13, July 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:121, July 19, 2005 **Ubuntu Security Notice, USN-152-1, July 21, 2005**
Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. A fixed version (5.8.4 or later) is available at: http://www.perl.com/CPAN/src/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandrake: http://www.mandrakesecure.net/en/ftp.php HP: http://software.hp.com/ **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005 HP Security Bulletin, HPSBUX01208, June 16, 2005 **Secunia, Advisory: SA16193, July 25, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; **zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6**	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update

	OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **zsync:** **http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download** Currently we are not aware of any exploits for this vulnerability.			Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 **Security Focus, 14162, July 21, 2005** **USCERT Vulnerability Note VU#680620, July 22, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc Debian Linux 3.1, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005

Multiple Vendors dhcpcd 1.3.22	A vulnerability has been reported in dhcpcd that could let a remote user perform a Denial of Service. Debian: http://security.debian.org/pool/updates/main/d/dhcpcd/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200507-16.xml **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/ index.php?id=a&anuncio=000983** Currently we are not aware of any exploits for this vulnerability.	dhcpcd Denial of Service CAN-2005-1848	Low	Secunia, Advisory: SA15982, July 11, 2005 Debian Security Advisory, DSA 750-1, July 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:117, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-16, July 15, 2005 **Conectiva, CLSA-2005:983, July 25, 2005**
Multiple Vendors KDE kopete 0.9-0.9.3, 3.4, 3.4.1, 3.3-3.3.2, 3.2.3; Wojtek Kaniewski ekg 1.1-1.6 rc1&rc2, 2005-06-05 22:03, 2005-04-11	Multiple vulnerabilities have been reported in 'libgadu.c' due to input validation errors and an integer overflow, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. EKG http://dev.null.pl/ekg/download.php KDE: ftp://ftp.kde.org/pub/kde/security_patches/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.355986 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200507-23.xml Currently we are not aware of any exploits for these vulnerabilities.	EKG 'LIbGadu' Multiple Vulnerabilities CAN-2005-1852	High	Security Tracker Alert ID: 1014539, July 21, 2005 Secunia, Advisory: SA16194, July 25, 2005 Slackware Security Advisory, SSA:2005-203-02, July 22, 2005 Gentoo Security Advisory, GLSA 200507-23 kopete, July 25, 2005
netpbm V10.0	A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code. No workaround or patch available at time of publishing. There is no exploit code required.	netpbm Arbitrary Code Execution	High	Secunia Advisory: SA16184, July 25, 2005
Netquery V3.1	Multiple vulnerabilities have been reported in Netquery that could allow a remote malicious user to perform cross site scripting, execute arbitrary code, or disclose information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Netquery Multiple Vulnerabilities	High	Security Focus, 14373, July 25, 2005
ProFTPd	Multiple format string vulnerabilities have been reported in ProFTPd that could let remote malicious users cause a denial of service or disclose information. Upgrade to version 1.3.0rc2: http://www.proftpd.org/ Currently we are not aware of any exploits for this vulnerability.	ProFTPD Denial of Service or Information Disclosure	Medium	Secunia, Advisory: SA16181, July 26, 2005
pstotext V1.9	A vulnerability has been reported in pstotext ('-dSAFER') that could let malicious users execute arbitrary postscript code. No workaround or patch available at time of publishing. There is no exploit code required.	pstotext Arbitrary Code Execution	High	Secunia, Advisory: SA16183, July 25, 2005
Raxnet Cacti 0.x	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'config_settings.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported in 'congif_settings.php' due to insufficient sanitization of the 'config[include_path]' parameter and in 'top_graph_header.php' due to insufficient sanitization of the 'config[library_path]' parameter, which could	RaXnet Cacti Multiple Input Validation CAN-2005-1524 CAN-2005-1525 CAN-2005-1526	High	Secunia Advisory: SA15490, June 23, 2005 Gentoo Linux Security Advisory, GLSA 200506-

	let a remote malicious user execute arbitrary code. Upgrades available at: http://www.cacti.net/download_cacti.php Gentoo: http://security.gentoo.org/glsa/glsa-200506-20.xml Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000978 SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/updates/main/c/cacti/** An exploit script has been published.			20, June 22, 2005 Conectiva Security Advisory, CLSA-2005:978, July 7, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 **Debian Security Advisory, DSA 764-1, July 21, 2005**
Raxnet Cacti prior to 0.8.6f	Multiple SQL injection vulnerabilities have been reported in the input filters due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in the 'graph_image.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported because 'session_start()', and 'addslashes()' can be prevented from being called due to a design error, which could let a remote malicious user obtain administrative access. Upgrades available at: http://www.cacti.net/download_cacti.php **Debian:** **http://security.debian.org/pool/updates/main/c/cacti/** There is no exploit code required.	RaXnet Cacti Multiple Vulnerabilities CAN-2005-2148 CAN-2005-2149	High	Hardened - PHP Project Security Advisory, July 1, 2005 **Debian Security Advisory, DSA 764-1, July 21, 2005**
SCO UnixWare Portmapper	A vulnerability has been reported in UnixWare Portmapper that could let remote malicious users cause a denial of service. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	UnixWare Portmapper Denial of Service CAN-2005-2132	Low	Security Focus, 14360, July 25, 2005
Shorewall Shorewall 2.0.x, 2.2.x, 2.4.x	A vulnerability has been reported due to a failure to properly implement expected firewall rules for MAC address-based filtering, which could let a remote malicious user bypass firewall rules. Hotfixes available at: http://www.shorewall.net/ **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	Shorewall MACLIST Firewall Rules Bypass CAN-2005-2317	Medium	Secunia Advisory: SA16087, July 18, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:123, July 21, 2005**
Vim V6.3.082	A vulnerability has been reported in Vim that could let remote malicious users execute arbitrary code. Vendor patch available: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.082 There is no exploit code required; however, Proof of Concept exploits have been published.	Vim Arbitrary Code Execution CAN-2005-2368	High	Security Focus, 14374, July 25, 2005

xine gxine 0.4.0-0.4.4	A format string vulnerability has been reported due to insecure implementation of a formatted printing function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200505-19.xml **Slackware:** **http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.360040** Currently we are not aware of any exploits for this vulnerability.	GXINE Remote Hostname Format String CAN-2005-1692	High	pst.advisory, May 21, 2005 Gentoo Linux Security Advisory, GLSA 200505-19, May 26, 2005 **Slackware Security Advisory, SSA:2005-203-04, July 22, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
3Com OfficeConnect Wireless 11g Access Point	A vulnerability has been reported in OfficeConnect Wireless 11g Access Point which could let malicious users disclose information. Update to 1.03.12: http://webprd1.3com.com/swd/jsp/ user/index.jsp?id=OCWAP15 There is no exploit code required.	3Com Wireless Access Point Information Disclosure CAN-2005-2391	Medium	Secunia, Advisory: SA16207, July 25, 2005
All Enthusiast, Inc. ReviewPost 2.0	An SQL injection vulnerability has been reported in 'Showproduct.PHP' due to insufficient sanitization of the 'sort' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	All Enthusiast ReviewPost 'Showproduct.PHP' SQL Injection	High	Secunia Advisory: SA16134, July 20, 2005
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious user to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000982 Currently we are not aware of any exploits for these vulnerabilities.	Apache HTTP Request Smuggling Vulnerability CAN-2005-1268 CAN-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005
ASN Guestbook V1.5	A vulnerability has been reported in ASN Guestbook that could allow remote malicious users to conduct cross site scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	ASN Guestbook Cross Site Scripting	High	Secunia, Advisory: SA16202, July 25, 2005
Atomic Photo Album V1.0.5	A vulnerability has been reported in Atomic Photo Album ('apa_module_basedir' in apa_phpinclude.inc.php) that could allow remote malicious user to include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Atomic Photo Album Arbitrary File Inclusion	High	Secunia, Advisory: SA16201, July 26, 2005
Blue Coat Systems All CacheOS systems, SGOS systems (SGOS 2.1.11 and earlier, SGOS 3.2.4 and earlier, SGOS 4.1.1), All SGME systems, All Spyware Interceptor systems	A remote Denial of Service vulnerability has been reported due to insufficient validation of TCP sequence numbers in ICMP error messages. SGOS 3.2.5: http://download.bluecoat.com/ release/SGOS3/index.html SGOS 4.1.2: http://download.bluecoat.com/ release/SGOS4/index.html Currently we are not aware of any exploits for these vulnerabilities.	Blue Coat TCP ICMP Message Sequence Numbers Denial of Service CAN-2005-0065 CAN-2005-0066 CAN-2005-0067 CAN-2005-0068	Low	Security Tracker Alerts, 1014531, 1014532, 1014533, & 1014534, July 20, 2005
CMSimple Content Management System 2.4 Beta 1- Beta 5, 2.4 Beta, 2.3, Beta 1- Beta 5, 2.2, Beta 1-Beta 4, 2.1, 2.0 Beta 1- Beta 4, 1.3 Beta 1 & Beta 2, 1.0-1.2 , Beta 1	A Cross-Site Scripting vulnerability has been reported in 'Index.php' due to insufficient sanitization of the 'search' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://www.cmsimple.dk/forum/viewtopic.php?	CMSimple Cross Site Scripting CAN-2005-2392	High	Security Focus, 14346, July 21, 2005

& 2	t=2470 There is no exploit code required; however, a Proof of Concept exploit script has been published.			
CMSimple V2.4	An input validation vulnerability has been reported in CMSimple ('index.php') that could let remote malicious users perform cross site scripting. Vendor fix available: http://www.cmsimple.dk/ forum/ viewtopic.php ?t=2470 There is no exploit code required.	CMSimple Cross Site Scripting	High	SecurityTracker, Alert ID: 1014556, July 22, 2005
Contrexx below V1.0.5	An input validation vulnerability has been reported in Contrexx that could let remote malicious users perform SQL injection or cross site scripting. A vendor update is available: http://www.contrexx.com/ There is no exploit code required; however, Proof of Concept exploits have been published.	Contrexx SQL Injection or Cross Site Scripting	High	SecurityTracker, Alert ID: 1014554, July 22, 2005
CreativePHP FormSender 1.0	A Cross-Site Scripting vulnerability has been reported in the 'Processform.PHP3' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	CreativePHP Cross Site Scripting	High	Security Focus 14324, July 19, 2005
CutePHP Team CuteNews 1.3.6	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'login.php' and 'search.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an installation path disclosure vulnerability was reported when a remote malicious user submits a certain URL. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	CuteNews Cross-Site Scripting & Path Disclosure CAN-2005-2393 CAN-2005-2394	High	Security Tracker Alert ID: 1014514, July 19, 2005
dxxo dxxo Count Web Statistics	An SQL injection vulnerability has been reported in the 'StatDay.asp,' 'StatMonth.asp,' and 'StatMonth.asp' scripts due to insufficient sanitization of the 'QDay,' 'QMonth,' and 'QYear' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	DXXO Count Web Statistics Multiple SQL Injection	High	Security Focus, 14341, July 21, 2005
ECI Telecom B-FOCuS Router 312+	A vulnerability has been reported in B-FOCuS Router that could let remote malicious users to obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	B-FOCuS Router Unauthorized Access	High	Security Focus, 14364, July 25, 2005
Free Host Shop Website Generator 3.3	Several vulnerabilities have been reported: a vulnerability was reported because a remote malicious user can use the image upload feature to upload a file containing arbitrary PHP code but having a '.jpeg' extension, which could lead to the execution of arbitrary PHP code; a Cross Site Scripting vulnerability was reported due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because a remote malicious user can supply an arbitrary UTL to obtain the installation path. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Free Host Shop Website Generator Remote Vulnerabilities	High	Security Tracker Alert ID: 1014535, July 20, 2005
FTPlocate V2.02	A vulnerability has been reported in FTPlocate that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required.	FtpLocate Arbitrary Command Execution	High	SecurityTracker, Alert ID: 1014570, July 25, 2005
Greasemonkey Greasemonkey 0.3.3	Multiple information disclosure vulnerabilities have been reported in the 'GM_xmlhttpRequest(),' 'GM_setValue(),' and 'GM_scripts()' functions due to a design error, which could let a remote malicious user obtain sensitive information. Update available at: http://atrus.org/hosted/ greasemonkey-0.3.5.xpi Proofs of Concept exploits have been published.	Greasemonkey Multiple Remote Information Disclosure	Medium	Security Focus, 14336, July 20, 2005

iTop10.Net PHP TopSites FREE 2.x, PHP TopSites PRO 2.x	A vulnerability has been reported in the 'setup.php' script, which could let a remote malicious user access the administration section without authentication. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHP TopSites Authentication Bypass	High	Secunia Advisory: SA16172, July 22, 2005
Mozilla Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/glsa-200507-14.xml Mandriva: http://www.mandriva.com/security/advisories **Gentoo:** **http://security.gentoo.org/glsa/glsa-200507-17.xml** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-586.html** **Slackware:** **http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880** Exploits have been published.	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 **Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005** **Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005** **RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005** **Slackware Security Advisory, SSA:2005-203-01, July 22, 2005**
Mozilla Firefox 1.0.5, 1.0.4	A vulnerability has been reported because basic authentication is chosen by default even if other authentication schemas are available, which would result in authentication credentials sent in plaintext format. No workaround or patch available at time of publishing. There is no exploit code required.	Mozilla Firefox Weak Authentication CAN-2005-2395	Medium	Security Focus 14325, July 19, 2005

Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, 7.0-7.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ Mandriva: http://www.mandriva.com/security/advisories FedoraLegacy: http://download.fedoralegacy.org/redhat/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.29 Gentoo: http://security.gentoo.org/glsa/glsa-200507-17.xml **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/**	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 US-CERT VU#519317 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Ubuntu Security Notice, USN-124-1 & USN-124-2, May 11 & 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005 Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005 PacketStorm, May 23, 2005 SCO Security Advisory, SCOSA-2005.29, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 **Fedora Update Notifications, FEDORA-2005-604 & 605, July 20, 2005**

	An exploit script has been published.			
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-434.html http://rhn.redhat.com/errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/ free/security/advisories/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 SGI Security Advisory, 20050503-01-U, June 8, 2005 SUSE Security Announcement, SUSE-SA:2005:030, June 9, 2005
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2; K-Meleon 0.9	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. RedHat: http://rhn.redhat.com/errata/ RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html Slackware: http://www.mozilla.org/projects/security/known-vulnerabilities.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/ free/security/advisories/ Mandriva:	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988, April 16, 2005 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 Slackware Security Advisory, SSA:2005-111-04, April 22, 2005 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U,

http://www.mandriva.com/security/advisories FedoraLegacy: http://download.fedoralegacy.org/redhat/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.29 Gentoo: http://security.gentoo.org/glsa/glsa-200507-17.xml **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required; however, a Proof of Concept exploit has been published.	May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005 Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005 SCO Security Advisory, SCOSA-2005.29, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 **Fedora Update Notifications, FEDORA-2005-604 & 605, July 20, 2005**

Multiple Vendors Windows XP, Server 2003 Windows Services for UNIX 2.2, 3.0, 3.5 when running on Windows 2000 Berbers V5 Release 1.3.6 AAA Intuit LX, Converged Communications Server (CCS) 2.x, MN100, Modular Messaging 2.x, S8XXX Media Servers	An information disclosure vulnerability has been reported that could let a remote malicious user read the session variables for users who have open connections to a malicious telnet server. Updates available: http://www.microsoft.com/tech net/security/Bulletin/MS05-033.mspx RedHat: ftp://updates.redhat.com/enterprise Microsoft: http://www.microsoft.com/tech net/security/Bulletin/MS05-033.mspx SUSE: ftp://ftp.SUSE.com/pub/SUSE AAA: http://support.avaya.com/elmodocs2/security/ASA-2005-145 RHSA-2005-504.pdf Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-567.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Mandriva: http://www.mandriva.com/security/advisories Microsoft: Bulletin revised to communicate the availability of security updates for Services for UNIX 2.0 and Services for UNIX 2.1. The “Security Update Information” section has also be revised with updated information related to the additional security updates. **F5:** **http://tech.f5.com/home/bigip/solutions/advisories/ sol4616.html** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Telnet Client Information Disclosure CAN-2005-1205 CAN-2005-0488	Medium	Microsoft, MS05-033, June 14, 2004 US-CERT VU#800829 iD EFENSE Security Advisory, June 14, 2005 Red Hat Security Advisory, RHSA-2005: 504-00, June 14, 2005 Microsoft Security Bulletin, MS05-033 & V1.1, June 14 & 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005 AAA Security Advisory, ASA-2005-145, June 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 SGI Security Advisories, 20050605-01-U, 20050702-01-U, & 20050703-01-U, July 12 & 15, 2005 Microsoft Security Bulletin, MS05-033 V2.0 July 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:119, July 14, 2005
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32,	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail /security -announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/ nph-reg3rdpty1.pl/product=05529& platform=osx&method=sa/SecUpd 2005-003Pan.dmg Debian: http://security.debian.org/pool/ updates/main/n/netkit-telnet/ Fedora:	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908

4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386 SGI IRIX 6.5.24-6.5.27	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/ CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/ document.do?assetkey= 1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/ en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/		Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005 SGI Security Advisory, 20050405-01-P, May 26, 2005 Debian Security Advisory, DSA 731-1, June 2, 2005 Conectiva Security Advisory, CLSA-2005:962, June 6, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Avaya Security Advisory, ASA-2005-132, June 14, 2005 **Fedora Legacy Update Advisory, FLSA:152583, July 11, 2005**

	elmodocs2/security/ ASA-2005-088 RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/ glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ ia32/ Sun: http://sunsolve.sun.com/ search/ document.do? assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/ Owl/CHANGES- current.shtml SCO: ftp://ftp.sco.com/pub/ updates/ OpenServer/ SCOSA-2005.23 SGI IRIX: Apply patch 5892 for IRIX 6.5.24-6.5.27: ftp://patches.sgi.com/ support/free/security/ patches/ Debian: http://security.debian.org/ pool/updates/main/k/krb4/ Conectiva: http://distro.conectiva.com .br/ atualizacoes/ index.php?id= a&anuncio=000962 Trustix: ftp://ftp.trustix.org/pub/ trustix/ updates/ Avaya: http://support.avaya.com/ elmodocs2/security/ ASA-2005-132 RHSA-2005-327.pdf **FedoraLegacy: http://download. fedoralegacy. org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors MediaWiki 1.4.6 & prior; Gentoo Linux	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads. sourceforge.net/ wikipedia/mediawiki- 1.4.7.tar.gz?do wnload Gentoo: http://security.gentoo.org/ glsa/glsa-200507-18.xml There is no exploit code required.	MediaWiki Remote Cross-Site Scripting CAN-2005-2396	High	Security Focus, 14327, July 20, 2005 Gentoo Linux Security Advisory, GLSA 200507-18, July 20, 2005
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/ warp/ public/707/cisco- sa- 20050412- icmp.shtml IBM:	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	US-CERT VU#222750 Sun(sm) Alert Notification, 57746, April 29, 2005 US-CERT VU#415294 Security Focus,

	ftp://aix.software.ibm.com/aix/efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1 ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. HP: www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU0116 **HP:** **www2.itrc.hp.com/service/ cki/docDisplay.do?docId=HPSBTU01210** Currently we are not aware of any exploits for these vulnerabilities.			13124, May 21, 2005 HP Security Bulletin, HPSBTU01210, July 17, 2005 **HP Security Bulletin, HPSBUX0116 Rev 4, July 19,2005**
MySQL AB MySQL 4.0 .0-4.0.11, 5.0 .0-5.0.4	A vulnerability has been reported in the 'mysql_install_db' script due to the insecure creation of temporary files, which could let a malicious user obtain unauthorized access. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/** There is no exploit code required.	MySQL 'mysql_install_db' Insecure Temporary File Creation CAN-2005-1636	Medium	Security Focus, 13660, May 17, 2005 **Fedora Update Notification, FEDORA-2005-557, July 20, 2005**
NETonE phpBook V1.46	An input validation vulnerability has been reported in phpBook that could let remote malicious users perform cross site scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	NETonE phpBook Cross Site Scripting CAN-2005-2397	High	SecurityTracker, Alert ID: 1014573, July 26, 2005
Oray PeanutHull 3.0 Beta 5	A vulnerability has been reported because SYSTEM privileges are not dropped before running another external program, which could let a malicious user execute arbitrary code with SYSTEM privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Oray PeanutHull System Privileges CAN-2005-2382	High	Secunia Advisory: SA16124, July 20, 2005
PHP FirstPost	A vulnerability has been reported in PHP FirstPost ('block.php') that could let remote malicious users execute arbitrary commands. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	PHP FirstPost Arbitrary Command Execution	High	SecurityTracker, Alert ID: 1014563, July 24, 2005
PHP Surveyor PHP Surveyor 0.98	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of the 'sid,' 'start,' 'id,' and 'lid' parameters, which could let a remote malicious user execute arbitrary SQL code; multiple Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a path disclosure vulnerability has been reported in certain scripts. No workaround or patch available at time of publishing. There is no exploit code required.	PHP Surveyor Multiple SQL Injection, Cross-Site Scripting & Path Disclosure CAN-2005-2381 CAN-2005-2380 CAN-2005-2398 CAN-2005-2399	High	Secunia Advisory: SA16123, July 20, 2005
PHPFinance PHPFinance 0.3	A vulnerability has been reported in 'Inc.login.php' due to an error, which could let a remote malicious user bypass authentication restrictions. Upgrades available at: http://prdownloads.sourceforge.net/phpfinance/phpfinance0.4.zip There is no exploit code required.	PHPFinance Inc.login.PHP Authentication Bypass CAN-2005-2400	Medium	Secunia Advisory: SA13276, July 19, 2005

PHP-Fusion PHP-Fusion 6.0.105, 6.0 106, 5.0 1 Service Pack, 5.0, 4.0 1, 4.00	A vulnerability has been reported due to insufficient verification of input passed to the BBCode 'color' tag before used in a post, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	PHP-Fusion BBcode 'Color' Tag Code Injection CAN-2005-2401	High	Security Focus, 14332, July 20, 2005
PHPNews PHPNews 1.2.3-1.2.6	An SQL injection vulnerability has been reported in 'Auth.php' due to insufficient sanitization of the 'user' and 'password' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHPNews 'Auth.PHP' SQL Injection CAN-2005-2383	High	Secunia Advisory: SA16148, July 21, 2005
PHPSiteSearch PHPSiteSearch 1.7.7 d	A Cross-Site Scripting vulnerability has been reported in 'Search.php' due to insufficient sanitization of the 'query' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	PHPSiteSearch 'Search.PHP' Cross-Site Scripting CAN-2005-2402	High	Secunia Advisory: SA16156, July 21, 2005
Project: Beehive Forum Beehive Forum V0.6RC2	Multiple vulnerabilities have been reported in Beehive Forum that could allow remote malicious users to perform SQL injection or cross site scripting. No workaround or patch available at time of publishing. There is no exploit code required.	Beehive Forum SQL Injection or Cross Site Scripting	High	Security Focus, 14361, 14363, July 25, 2005
Pyrox Search Pyrox Search 1.0.5	A Cross-Site Scripting vulnerability has been reported in 'Newsearch.PHP' due to insufficient sanitization of the 'Whatdoreplace' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Pyrox Search 'Newsearch.PHP' Cross-Site Scripting	High	Secunia Advisory: SA16154, July 21, 2005
RealChat Software RealChat V3.5.1b	A vulnerability has been reported in RealChat that could let remote malicious users impersonate other users. No workaround or patch available at time of publishing. There is no exploit code required.	RealChat User Impersonation CAN-2005-2403	Medium	Security Focus, 14358, July 23, 2005
SAP Internet Graphics Server V6.40	An input validation vulnerability has been reported in Internet Graphics Server that could let remote malicious users traverse directories. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits have been published.	Internet Graphics Server Directory Traversal CAN-2005-1691	Medium	Secunia, Advisory: SA16208, July 25, 2005
Sendcard V3.2.3	A vulnerability has been reported in Sendcard ('id') that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	Sendcard SQL Injection CAN-2005-2404	High	Secunia, Advisory: SA16165, July 22, 2005
Siemens Santis 50 Wireless Router V4.2.8.0	A vulnerability has been reported in Santis 50 Wireless Router that could let remote malicious users perform a denial of service. No workaround or patch available at time of publishing. There is no exploit code required.	Siemens Wireless Router Denial Of Service	Low	Security Focus, 13679, July 25
Tim Hoeppner Ultimate PHP Board 1.9.6, 1.9, 1.8.2, 1.8, 1.0 b, 1.0 final beta, 1.0	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'send.php,' 'users.php,' 'top.php,' and 'main.php' due to insufficient sanitization of the 'css' parameter, and in 'header.php' due to insufficient sanitization of the 'title' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'index.php' and 'register.php' due to insufficient sanitization of the 'User-Agent' HTTP header, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Tim Hoeppner Ultimate PHP Board Multiple Cross-Site Scripting	High	Secunia Advisory: SA16144, July 21, 2005
Xerox WorkCentre & WorkCentre Pro MicroServer Web Server	Multiple vulnerabilities have been reported in MicroServer Web Server that could allow users unauthorized access, perform cross site scripting, or cause a denial of service. Vendor fix available: http://www.xerox.com/downloads/ usa/en/c/cert_XRX05_007.pdf Currently we are not aware of any exploits for these vulnerabilities.	Xerox MicroServer Web Server Multiple Vulnerabilities	High	Secunia, Advisory: SA16167, July 22, 2005 Xerox Security Bulletin XRX05-007, July 18, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Congress to take up VoIP 911 rules in September:** The U.S. Senate and House of Representatives in May introduced a joint measure that would require all voice over Internet Protocol providers connected to the public telephone network to link up customers to the 911 network as well. They expect to begin hearings on its proposed 911 service requirements for VoIP providers in September. Source: http://news.zdnet.com/2100-1035_22-5798665.html.

Wireless Vulnerabilities

- **weplab-0.1.5_win32.zip:** A tool to review the security of WEP encryption in wireless networks. Several attacks are included. See Script/Technique Table entry below.
- **Dedicated Mobile Services Carry Out Anonymous Web Attacks:** Various Mobile Services provide malicious users with an intermediate point to anonymously browse web resources and execute attacks against them. An attacker can take advantage of the Google's WMLProxy Service by sending a HTTP GET request with carefully modified URL of a malicious nature. Such request hides the attacker's IP address and may slow down future investigations on a successful break-in since Google's Services are often over-trusted. Source: http://www.securiteam.com.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
July 23, 2005	icmp-tools.tgz	Yes	Exploits for Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service vulnerability
July 23, 2005	47slimftpd_bof.pl.txt	Yes	Proof of concept exploit for SlimFTPd Arbitrary Code Execution vulnerability
July 22, 2005	netquery31.txt	No	Exploit for Netquery Multiple Vulnerabilities
July 22, 2005	advisory_112005.59.txt	Yes	Proof of concept exploit for Contrexx SQL Injection or Cross Site Scripting vulnerability
July 21, 2005	weplab-0.1.5_win32.zip	N/A	A tool to review the security of WEP encryption in wireless networks from an educational point of view that includes several attacks so it can measure the effectiveness and minimum requirements of each one. Currently, weplab supports several methods, and it is able to crack the WEP key from 600,000 encrypted packets.
July 21, 2005	Return-to-libc.txt	N/A	A whitepaper that discusses the return of libc attacks used to bypass non-executable stacks.
July 21, 2005	mobileTraverse.txt	N/A	Misuse of services like Google's WMLProxy and IYHY allow for proxied/anonymous attacks against web sites.
July 21, 2005	Intruder-exp.pl	No	Script that exploits the Intruder Client Remote Denial of Service vulnerability.
July 21, 2005	icc_ex.c	No	Proof of Concept exploit for the MS05-03 JPEG ICC overflow vulnerability.
July 21, 2005	Greasemonkey.txt	Yes	Exploit for the Greasemonkey Multiple Remote Information Disclosure vulnerability.
July 21, 2005	CMSimpleXSS.txt	Yes	Proof of Concept exploit for the CMSimple 'Index.PHP' Cross-Site Scripting vulnerability
July 20, 2005	GoogleBam.txt	N/A	A remote malicious user can mask their origin IP address because Google allows for proxy based attacks via WML servers.
July 19, 2005	javaprxy.pl	Yes	Proof of Concept exploit for the Microsoft Windows Color Management Module Buffer Overflow or Arbitrary Code Execution vulnerability.

[back to top]

Trends

- **Survey: Americans guard against ID theft:** According to a poll conducted by Money magazine and ICR, the majority of Americans fear the threat of identity theft and are doing something about it. The telephone poll, which surveyed a little more than 1,000 individuals in June, revealed that 78 percent of those interviewed expressed concern that their identity may be stolen. Only 8 percent of those interviewed claimed to have been a victim of identity theft. Ninety-six percent of Americans said they have taken some precautionary measure to protect their personal information. Source: http://money.cnn.com/2005/07/18/pf/security_identity_poll/index.htm?section=money_latest.
- **Internet users ignorant about data privacy:** According to a study titled "Open to Exploitation: American Shoppers Online and Offline," Internet users in the United States are ignorant about the type of data that Website owners collect from them and how that data is used. This makes them vulnerable to fraud and misuse of their personal information. Source: http://www.infoworld.com/article/05/07/18/HNdataprivacy_1.html?source=rss&url=http://www.infoworld.com/article/05/07/18/HNdataprivacy_1.html.
- **Cost of US cyber attacks plummets:** The 10th annual Computer Crime and Security Survey, put together by the Computer Security Institute (CSI) in conjunction with information security experts at the FBI shows that the cost of individual cyber attacks fell dramatically in the US last year but unauthorized access and the theft of proprietary information remain top security concerns. Virus attacks continue as the source of the greatest financial pain, making up 32 per cent of the overall losses reported. Source: http://www.theregister.co.uk/2005/07/18/csi_fbi_security_survey/.
- **iTunes IM worm drops adware:** A new version of the Opanki worm has been discovered. The instant messaging worm masquerades as Apple Computer's iTunes application and drops adware on infected Windows PCs. Source: http://news.zdnet.com/2100-1009_22-5797170.html?tag=zdfd.newsfeed.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win 32 Worm	Slight Increase	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win 32 Worm	Increase	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Mytob.c	Win 32 Worm	Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
4	Netsky-Q	Win 32 Worm	Slight Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
4	Mytob-BE	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Lovgate.w	Win 32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
6	Netsky-Z	Win 32 Worm	Increase	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
6	Mytob-AS	Win 32 Worm	New	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
9	Netsky-D	Win 32 Worm	Decrease	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
10	Mytob-EP	Win 32 Worm	New	June 2005	Another slight variant of the mass-mailing worm that utilizes an IRC backdoor and LSASS vulnerability to propagate. Also propagates by email, harvesting addresses from the Windows address book.

Table updated July 24, 2005

Viruses or Trojans Considered to be a High Level of Threat

- Nothing Significant to Report.

[back to top

Last updated July 29, 2005